RECEIVED
CENTRAL FAX CENTER
JAN 05 2007

FAX COVER SHEET

PLEASE CONFIRM RECEIPT OF THIS FACSIMILE

DIRECTV

Attention:	MAIL STOP APPEAL BRIEF - PATENTS Group Art Unit: 2134 Examiner: Matthew E. Heneghan	Fax:	(571) 273-8300
UNITED STATES PATENT AND TRADEMARK OFFICE		Phone:	(571) 272-3834
Pages:	Cover + 1 + 1 + 1 + 21 = 25	Date:	January 5, 2007
From:	Georgann S. Grunebach	Fax:	(310) 964-0941
	Assistant General Counsel	Phone:	(310) 964-4615

CERTIFICATION OF FACSIMILE TRANSMISSION UNDER 37 CFR 1.8

I hereby certify that this correspondence identified below is being facsimile transmitted to (571) 273-8300 (Centralized Facsimile Number), addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on January 5, 2007.

Georgann S. Grunebach, Reg. No. 33,179 — January 5, 2007
(Printed Name of Person Signing Certificate) — (Date of Signature)

Telephone No. (310) 964-4615

Attention: Commissioner for Patents **Attorney Docket No. PD-201161**

Please find attached Re: 10/085,860 Filing Date: February 28, 2002

- TRANSMITTAL FORM PTO/SB/21 (1 page)
- FEE TRANSMITTAL FORM PTO/SB/17 (1 page in duplicate)
- BRIEF OF APPELLANTS (21 pages)

PLEASE CONFIRM RECEIPT OF THIS FACSIMILE

If you do not receive all pages, or pages are not clear, please call Karen Lum at (310) 964-0735.

The DirecTV Group, Inc., CA/LA1/A109, P. O. Box 956, El Segundo CA 90245

RECEIVED
CENTRAL FAX CENTER
JAN 05 2007

PTO/SB/21 (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission: 24

Application Number	10/085,860
Filing Date	February 28, 2002
First Named Inventor	Ronald P. Cocchi
Art Unit	2134
Examiner Name	HENEGHAN, Matthew E.
Attorney Docket Number	PD-201161

ENCLOSURES (Check all that apply)

- [x] Fee Transmittal Form
  - [ ] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) _____
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [x] Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	The DirecTV Group, Inc.		
Signature			
Printed name	Georgann S. Grunebach		
Date	January 5, 2007	Reg. No.	33,179

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature			
Typed or printed name	Georgann S. Grunebach	Date	January 5, 2007

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

JAN 0 5 2007

PTO/SB/17 (07-06)
Approved for use through 01/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995 no persons are required to respond to a collection of information unless it displays a valid OMB control number

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL For FY 2006

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 500

Complete if Known	
Application Number	10/085,860
Filing Date	February 28, 2002
First Named Inventor	Ronald P. Cocchi
Examiner Name	HENEGHAN, Matthew E.
Art Unit	2134
Attorney Docket No.	PD-201161

METHOD OF PAYMENT (check all that apply)

☐ Check ☐ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): _____

☑ Deposit Account Deposit Account Number: 50-0383 Deposit Account Name: The DIRECTV Group, Inc.

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☑ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee ($)	FILING FEES Small Entity Fee ($)	SEARCH FEES Fee ($)	SEARCH FEES Small Entity Fee ($)	EXAMINATION FEES Fee ($)	EXAMINATION FEES Small Entity Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	
Design	200	100	100	50	130	65	
Plant	200	100	300	150	160	80	
Reissue	300	150	500	250	600	300	
Provisional	200	100	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims ____ - 20 or HP = ____ x Fee ($) ____ = Fee Paid ($) ____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims ____ - 3 or HP = ____ x Fee ($) ____ = Fee Paid ($) ____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims: Fee ($) ____ Fee Paid ($) ____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets ____ - 100 = Extra Sheets ____ / 50 = Number of each additional 50 or fraction thereof ____ (round up to a whole number) x Fee ($) ____ = Fee Paid ($) ____

4. OTHER FEE(S)

	Fees Paid ($)
Non-English Specification, $130 fee (no small entity discount)	
Other (e.g., late filing surcharge): Fee for filing a brief in support of an appeal	$500

SUBMITTED BY

Signature		Registration No. (Attorney/Agent) 33,178	Telephone 310-964-4615
Name (Print/Type)	Georgann S. Grunebach		Date January 5, 2007

RECEIVED
CENTRAL FAX CENTER
JAN 05 2007

Due Date: January 11, 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	)	
	)	
Inventor: Ronald P. Cocchi et al.	)	Examiner: Matthew E. Heneghan
	)	
Serial No.: 10/085,860	)	Group Art Unit: 2134
	)	
Filed: February 28, 2002	)	Appeal No.: _____
	)	
Title: ASYNCHRONOUS CONFIGURATION	)	

BRIEF OF APPELLANTS

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In accordance with 37 CFR §41.37, Appellants hereby submit the Appellants' Brief on Appeal from the final rejection in the above-identified application, as set forth in the Office Action dated August 15, 2006, and the Advisory Action dated October 27, 2006.

Please charge the amount of $500.00 to cover the required fee for filing this Appeal Brief as set forth under 37 CFR §41.37(a)(2) and 37 CFR §41.20(b)(2) to Deposit Account No. **50-0383** of The DirecTV Group, Inc. Also, please charge any additional fees or credit any overpayments to Deposit Account No. **50-0383**. Fee Transmittal Form PTO/SB/17 is enclosed in duplicate.

01/08/2007 TL0111 00000051 500383 10085860
01 FC:1402 500.00 DA

I. REAL PARTY IN INTEREST

The real party in interest is THE DIRECTV GROUP, INC., the assignee of the present application.

II. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences for the above-referenced patent application.

III. STATUS OF CLAIMS

Claims 1-10, 12-13, 15, 17-25, 27-28, 30-40, 42-43, 45, 47-55, and 57-58 remain in the application.

Claims 11, 14, 16, 26, 29, 41, 44, 46, 56, and 59 have been cancelled.

Claims 1-10, 15, 17-25, 30-40, 45, and 47-55 have been allowed.

Claims 12, 13, 27, 28, 42, 43, 57, and 58 stand rejected.

The rejection of claims 12, 13, 27, 28, 42, 43, 57, and 58 are being appealed.

IV. STATUS OF AMENDMENTS

Claims 1, 15, 30, and 45 were amended and claims 14, 29, 44, and 59 were cancelled subsequent to the final Office Action.

Pursuant to the Advisory Action dated October 27, 2006, all of the amendments were entered into the record.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claims 1, 15, 30, and 45 are generally directed to the use of a CAM/smart card to prevent unauthorized access to digital services (see paragraph [0005]-page 1, lines 9-22).

A control center (102) is configured to coordinate and provide digital services (see paragraph [0028] -page 5, lines 19-26 and FIG. 1). An uplink center 104 is configured to receive the digital services from the control center 102 and transmit the digital services to a satellite 108 (see paragraph [0028]-[0029] – page 5, line 19 to page 6, line 5; and FIG. 1). The satellite 108 is configured to receive the digital services from the uplink center 104, process the digital services, and transmit the digital

services and configuration information for accessing the digital services to a subscriber receiver station 110 (see paragraph [0029] –page 5, line 27-page 6, line 5; FIG. 1).

The subscriber receiver station 110 is configured to receive the digital services and configuration information from the satellite 108 and control access to the digital services through an integrated receiver/decoder (IRD) 126 (see paragraph [0030]-[0031]- page 6, lines 6-16).

A conditional access module (CAM) 512 is communicatively coupled to the (IRD) 126 (see FIG. 5 and paragraph [0030]- page 6, lines 6-11). The CAM 512 is configured to receive the configuration information that been transmitted asynchronously (see paragraph [0071]- page 17, lines 6-18; FIGs. 5 and 7).

The CAM 512 contains a custom logic block 610 that is configured to dynamically reconfigure a hardware state machine in the CAM 512 based on the configuration information (see paragraphs [0005]-page 5, lines 19-22, [0015]-page 4, lines 5-14, [0027]-page 5, lines 12-16, [0067]-page 16, lines 3-13, [0073]-page 18, lines 1-15, [0074]-page 18, lines 16-24, [0078]-page 19, lines 14-24, [0080]-page 20, lines 5-11, [0082]-page 20, line 22-page 21, line 5; FIGs. 5, 6, 7). The hardware state machine comprises custom logic 610 that is used to control access to the digital services (see paragraph [0066]-page 15, line 21-page 16, line 2, [0069]-page 16, lines 21-25; and FIG. 7). Further, the hardware state machine is not directly accessible to a system input/output module 608 or system bus 612 of the CAM 512 (see paragraph [0015]-page 4, lines 5-14, [0078]-page 19, lines 14-24; FIGS. 7 and 8). In addition, the custom logic block 610 comprises a dedicated hardware reconfiguration and input/output module 714 that connects the hardware state machine to a system bus 612 of the CAM 512 and controls access to logic of the hardware state machine (see paragraph [0069]-page 16, lines 21-25 and FIG. 7).

Thus, as claimed, since the hardware state machine is not accessible to the system input/output module or system bus of the CAM/smart card, and because the implementation is hardware based, it is protected from being altered by the microprocessor of the CAM/smart card or external means.

Dependent claim 12, 27, 42, and 57 provides that the custom logic block 610 comprises an asynchronous dynamic pre-permutation module that employs a series of one or more configurable multiplexors and the beginning of the hardware state machine 718 (see paragraphs [0070]-[0074] – page 16, line 26-page 18, line 24; FIG. 7).

Dependent claims 13, 28, 43, and 58 provide that the custom logic block comprises an asynchronous dynamic post-permutation module that employs a series of one or more configurable mutliplexors at the end of the hardware state machine 718 (see paragraphs [0070]-[0074] - page 16, line 26-page 18, line 24; FIG. 7).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 12, 13, 27, 28, 42, 43, 57, and 58 stand rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement.

Claims 12, 13, 27, 28, 42, 43, 57, and 58 stand rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural connections.

VII. ARGUMENTS

A. Claims 12, 13, 27, 28, 42, 43, 57, and 58 Are Enabled in Accordance with 35 U.S.C. §112, First Paragraph.

In the final Office Action, claims 12, 13, 27, 28, 42, 43, 57, and 38 were rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement.

More specifically, the claims were rejected stating that while the specification suggests the use of multiplexors with the hardware state machine, nowhere is it described in the manner in which the multiplexors are actually used or configured.

In the prior response, Appellants referred the Examiner to paragraphs [0070][0074]:

> **[0070]** The hardware state machine 718 may contain the same logic as used in the prior art and may not be modified. In addition to the state machine 718, the implementation consists of a permutation that employs a series of configurable multiplexors at the beginning 716 and end 720 of the fixed hardware state machine 718. Custom logic (i.e., the logic within hardware configuration control and IO module 714) interconnects the multiplexors (within permutations 716 and 720) to the system bus 612 of CAM 512. Accordingly, the hardware configuration control and IO module 714 that connects to the system bus 612 controls access to the permutation 716 and 720 and state machine 718 logic.
> **[0071]** The custom logic within the control and IO module 714 implements a key exchange protocol by accepting (or rejecting) a series of pre-authorized keys (e.g., sequentially wrapped keys with $n=10^6$ times or other large value) or other secure

protocol. The key defines a configuration for the permutations 716 and 720. Valid keys are only known to the headend (e.g., uplink center 104) by using any public key algorithm such as Rabin or RSA (Rivest-Shamir-Adelman). Based on a public key algorithm, the keys cannot be recreated or generated by unknown parties. The keys are delivered to the smart card either over the broadcast stream, Internet, or other appropriate distribution channel. The keys can be delivered to the smart card (i.e., CAM 512) population asynchronously (e.g., over a period of several hours, days, or months). The keys may be delivered using uniquely encrypted, group encrypted packets. These packets are unintelligible to members (i.e., CAMs 512) for which they were not encrypted. In other words, the packets are only intelligible to those members/control and IO modules 714 having the appropriate private key.

[0072] The hardware configuration control and IO module 714 verifies/authenticates the key. Such a verification/authentication may ensure that the key is from a known source (e.g., a known uplink center 104, program source 200A-200C,etc.), that the key is not a duplicate of an already received key, or that the key fails to comply with an additional security measure. As part of the authentication process, the control and IO module 714 decrypts the keys. The decrypted key is then verified/authenticated by the custom logic within module 714. If the key is valid, the key is retained by the control and IO module 714 (e.g., by storing the keys in protected registers with no physical or logical output mechanism outside the custom logic within the module 714). If the key is invalid, the key is rejected and may not be stored by the control and IO module 714.

[0073] As described above, the key defines a configuration for the permutations 716 and 720. Accordingly, when appropriate, the key is used to dynamically (i.e., on-the-fly) reconfigure the permutations 716 and 720. The timing of the reconfiguration may occur immediately upon receipt of the key. Alternatively, the key may be stored by control and IO module 714 and only used to reconfigure the permutations 716 and 720 (e.g., switch the configuration to that represented by the stored key) upon receipt of an over the air command. In such a circumstance, the control and IO module 714 may store a currently active key (that defines a permutation 716 and 720 currently being used) and a future key. Accordingly, the keys may be delivered asynchronously over a very long period of time to multiple CAMs 512 where they are validated and stored asynchronously. Thereafter (e.g., once a period of time has passed to ensure that appropriate/enough CAMs 512 have the new key), an over the air command to activate a reconfiguration operation for a key may be delivered synchronously to all CAMs 512. Thus, the actual reconfiguration operation may occur simultaneously within all CAMs 512, while the key delivery and validation mechanism is asynchronous over a period of time.

[0074] To reconfigure the permutations, 716 and 720, the control and IO module 714 communicates bi-directly 722 with the pre-permutations 716 and post-permutations 720 to dynamically configure the series of multiplexors in each respective permutation 716 and 720. Once configured, the pre-permutations 716 place the digital services information received across communication link 724 from control and IO module 714 into the appropriate form for use by the hardware state

> machine 718. Hardware state machine 718 may modify the digital services information based on custom logic within the state machine 718. Thereafter, the post-permutations 720 may modify the outgoing digital services information to limit use and viewing of the information from unauthorized attackers.

As can be seen, such paragraphs clearly provide that the key is used to configure the series of multiplexors within each permutation. The claims provide for using a series of configurable multiplexors based on the key. Since the multiplexors are configurable, the key may be used to dynamically configure the various components of the invention. Further, contrary to that asserted in the final Office Action, such a use clearly establishes how the multiplexors are used.

In addition, Appellants previously provided a standard dictionary definition for a multiplexor that described a rearrangement of elements of a set. Such a definition was merely ignored in the final Office Action. Appellants further referred to another definition from wikipedia – "http:en.wikipedia.org/wiki/Demultiplexor" to further evidence the state of the art of multiplexors and demultiplexors. The definition provides "It is usual to combine a multiplexor and a demultiplexor together into one piece of equipment and simply refer to the whole thing as a 'multiplexor'...". Based on such a definition, it is clearly that a multiplexor (that includes both a multiplexor and demultiplexor) can easily be configured to have inputs and outputs that merely permute the data. Nonetheless, the claims do not require an identical number of inputs and outputs as suggested by the Examiner. Instead, the pre-permutation module merely employs a series of configurable multiplexors while the post-permutation module also employs a series of configurable multiplexors. Such a teaching is completely clearly establishes sufficient support to practice the claimed invention.

In addition, Appellants submit that the use of configurable multiplexers are known in the art. For example, U.S. Patent No. 5,867,644 by Ranson describes the existence of configurable multiplexors and how such user configurable multiplexer circuitry can be used (See Abstract). Thus, the recitation in the present invention that describes the use of the key to configure the multiplexors in combination with the known use of configurable multiplexors clearly enables the practice of the invention. In addition, the invention provides unique features and advantages over that of the prior art.

The Advisory Action asserts that the specification paragraph 70 simply states that the invention connects multiplexers using custom logic. Appellants respectfully disagree and traverse such an assertion. Paragraph 70 is recited above and provides that a permutation employs a series of configurable multiplexors. Further, contrary to that asserted in the Office Action, paragraph 70 states that the custom logic interconnects the configurable multiplexors to the system bus of the CAM. Again, the custom logic utilizes these configurable multiplexors at the beginning and end of the hardware state machine. Further, the above paragraphs specify that a key is used to define the configuration for the multiplexors. The above paragraphs 70-74 provide and describe explicitly how the multiplexors are used in the invention and in fact provide enabling support under 35 U.S.C. 112.

In response to the above arguments, the Advisory Action mailed on October 27, 2006 provides:

> In reciting the definition from Wikipedia, Applicant has not entered the citation into the record. As previously stated, Applicant's arguments do not refute the case that Applicant's specification simply states that the invention connects multiplexers using "custom logic" (see paragraph 70), without suggesting what that logic is. There exist many designs for permutors that are well-known in the art. For any digital logic design, there exists a large number of alternative designs, using different types of gates, that would produce the same set of outputs from the same respective inputs. It is therefore reasonable to conclude that it would be possible, given an arrangement of a number of multiplexers, to derive an output that is a rearrangement of an input. It would not, however, be clear to one of ordinary skill in the art (i.e., a journeyman digital logic designer) how to implement such a functionality without having to perform undue experimentation. Applicant's reference to U.S. Patent No. 5,867,644 is not persuasive in that the multiplexers (see figures 45 and 46 and columns 28 and 29) are being used for a purpose (the configuration of a circuit test bed) that does not appear to be applicable to the non-deterministic permuting of data between a cryptographic I/O controller and a state machine as in Applicant's invention.

Appellants respectfully disagree with and traverse the above assertions. As can be seen from the above, the Examiner is asserting that a journeyman in the art would not know how to merely rearrange inputs into different outputs using multiplexers without undue experimentation. Such an assertion is wholly without merit. Nonetheless, regardless of the merit of such an assertion, Appellants note that such a permutation or rearrangement is not what is required by the claims.

In the prior response (as described above), Appellants addressed the enablement aspects of the invention with respect to the use of multiplexors. In addition, as stated above, Appellants directed the attention of the Examiner to multiple different definitions of a multiplexor from various sources. Such definitions were not needed nor used to establish the prior art. Accordingly, there was no need to enter the citation into the record. Rather, the definitions were merely used to indicate to the Examiner that the use of a multiplexor was in contrast to the definition used and asserted by the Examiner in this matter. Further, the definitions were used to establish that multiplexors in general are known in the art and their use need not be described in specific detail in a specification in order to enable the invention. Accordingly, Appellants have clearly established the existence and use of configurable multiplexors.

It is the Examiner's obligation to set forth a prima facie rejection. The Examiner has failed to establish that the use of multiplexors in the manner claimed are not enabled by the specification.

In the Advisory Action, the Examiner asserts:

> Applicant's arguments do not refute the case that Applicant's specification simply states that the invention connects multiplexers using 'custom logic' (see paragraph 70), without suggesting what that logic is.

Appellants respectfully disagree and traverse such an assertion. Appellants have referred multiple times to paragraphs [0070]-[0074] of the specification which clearly establish and describe how multiplexors are used. Paragraph [0071] describes the custom logic that utilizes a key that defines a configuration for permutations. Paragraphs [0072]-[0074] further describe such permutations. Again, as stated in the previously submitted arguments, the present claims do not recite nor specify that the same number of inputs or outputs are used. Instead, the claims provide for using a series of configurable multiplexors based on the key. Since the multiplexors are configurable, the key may be used to dynamically configure the various components of the invention. Such a use clearly establishes a how the multiplexors relate to the invention and how they are used.

In rejecting the claims, the Examiner is ignoring these paragraphs (i.e., paragraphs [0070]-[0074]) from the specification thereby establishing an omission of an essential element needed for a prima facie rejection under 35 U.S.C. §112 and resulting in clear error in the rejection.

In addition, the Examiner has indicated that U.S. Patent No. 5,867,644 is used for a different purpose from that of the present invention and therefore cannot be used to provide enabling support. Appellants note that the '644 reference was merely provided to make clear to the Examiner that configurable multiplexors are known in the art. The particular manner in which a multiplexor is configured is set forth in the present invention and claims. Accordingly, the end use for which the Examiner is relying has no relevance with respect to the present invention. Further, for 112 support, the field of invention is not particularly relevant. In this regard, the standard for determining whether an invention is enabled is whether the experimentation needed to practice the invention is undue or unreasonable (see MPEP 2164). Here, any person of ordinary skill in the art would know that multiplexors can be configurable. Accordingly, to argue that multiplexors cannot be configurable is wholly without merit and ignoring the clear standards set forth in the case law and MPEP.

Again, the specification clearly establishes and describes how multiplexors are connected and used. Namely, a permutation (which is defined using a key) employs a series of configurable multiplexors. The configurable multiplexors are used at the beginning and end of a hardware state machine. Again, the specification explicitly describes that a key is used to define the configuration for the multiplexors.

Such a citation and description in the specification clearly provides sufficient support under 35 U.S.C. §112. To fail to consider such a teaching establishes clear error in the Examiner's rejection and fails to consider an essential element needed for a 112 based rejection.

In view of the above, Appellants respectfully request that the rejections under 35 U.S.C. 112 be reversed and direct the Examiner to allow the claims.

B. Claims 12, 13, 27, 28, 42, 43, 57, and 58 Are Not Incomplete Under 35 U.S.C. §112, Second Paragraph.

In the final Office Action, claims 12, 13, 27, 28, 42, 43, 57, and 58 were rejected under 35 U.S.C. §112, second paragraph, as being incomplete for omitting essential structural cooperative relationships of elements, such omission amounting to a gap between the necessary structural

connections. More specifically, the rejection states that it is unclear how the multiplexors relate to the remainder of the invention.

The claims clearly recite that the custom logic block of the independent claims comprises either a pre-permutation module or a post-permutation module that employs a series of configurable multiplexors at the beginning or end of the hardware state machine of the custom logic block.

As described above, Appellants direct the attention of the Board to paragraphs [0070]-[0074] of the specification as filed (recited above). As can be seen, such paragraphs clearly provide that the key is used to configure the series of multiplexors within each permutation. The claims do not recite nor specify that the same number of inputs or outputs are used. Instead, the claims provide for using a series of configurable multiplexors based on the key. Since the multiplexors are configurable, the key may be used to dynamically configure the various components of the invention.

Thus, the mutliplexors are clearly claimed as part of the custom logic block that are used at the beginning or end of the hardware state machine within such a custom logic block. Such a use clearly establishes how the multiplexors relate to the invention. Accordingly, there are insufficient grounds to maintain a rejection under 35 U.S.C. §112, second paragraph.

Appellants further note that the rejection recites MPEP §2172.01 which provides:

> A claim which omits matter disclosed to be essential to the invention as described in the specification or in other statements of record may be rejected under 35 U.S.C. 112, first paragraph, as not enabling. *In re Mayhew*, 527 F.2d 1229, 188 USPQ 356 (CCPA 1976). See also MPEP § 2164.08(c). Such essential matter may include missing elements, steps or necessary structural cooperative relationships of elements described by the applicant(s) as necessary to practice the invention.
>
> In addition, a claim which fails to interrelate essential elements of the invention as defined by applicant(s) in the specification may be rejected under 35 U.S.C. 112, second paragraph, for failure to point out and distinctly claim the invention. See *In re Venezia*, 530 F.2d 956, 189 USPQ 149 (CCPA 1976); *In re Collier*, 397 F.2d 1003, 158 USPQ 266 (CCPA 1968). >But see *Ex parte Nolden*, 149 USPQ 378, 380 (Bd. Pat. App. 1965) ("[I]t is not essential to a patentable combination that there be interdependency between the elements of the claimed device or that all the elements operate concurrently toward the desired result"); *Ex parte Huber*, 148 USPQ 447, 448-49 (Bd. Pat. App. 1965) (A claim does not necessarily fail to comply with 35 U.S.C. 112, second paragraph where the various elements do not function simultaneously, are not directly functionally related, do not directly intercooperate, and/or serve independent purposes.).

RECEIVED
CENTRAL FAX CENTER
JAN 0 5 2007

In view of the above cited portion of the MPEP, the omitted structural elements must be essential to the invention in order to maintain the 112, second paragraph rejection. Appellants submit that the dependent claims do not omit any such essential elements. In this regard, the claims specify that configurable muiltiplexors are placed at the beginning or end of the hardware state machine. As described in section A above, such elements are clearly enabled by the specification. Further, there are no essential elements that are missing, nor are necessary structural cooperative relationships of the multiplexor use lacking.

Accordingly, Appellants respectfully request reversal of the rejections and further request that the Board direct the Examiner to allow the rejected claims.

CONCLUSION

In light of the above arguments, Appellants respectfully submit that the cited references do not anticipate nor render obvious the claimed invention. Further, all of the claims are in compliance with and fully enable the invention under 35 U.S.C. §112, first paragraph. As a result, a decision by the Board of Patent Appeals and Interferences reversing the Examiner and directing allowance of the pending claims in the subject application is respectfully solicited.

Respectfully submitted,

Attorneys for Appellant(s)

By: _____
Name: Georgann S. Grunebach
Reg. No.: 33,179

Date: January 5, 2007

The DIRECTV Group, Inc.
CA/LA1/A109
2230 E. Imperial Highway
P. O. Box 956
El Segundo CA 90245

Telephone No. (310) 964-4615

VIII. CLAIMS APPENDIX

1. (CURRENTLY AMENDED) A system for controlling access to digital services comprising:

(a) a control center configured to coordinate and provide digital services;

(b) an uplink center configured to receive the digital services from the control center and transmit the digital services to a satellite;

(c) the satellite configured to:

(i) receive the digital services from the uplink center;

(ii) process the digital services; and

(iii) transmit the digital services and configuration information for accessing the digital services to a subscriber receiver station;

(d) the subscriber receiver station configured to:

(i) receive the digital services and configuration information from the satellite;

(ii) control access to the digital services through an integrated receiver/decoder (IRD);

(e) a conditional access module (CAM) communicatively coupled to the (IRD), wherein the CAM is configured to receive the configuration information, and wherein the configuration information has been transmitted asynchronously; and

(f) a custom logic block within the CAM, wherein the custom logic block is configured to dynamically reconfigure a hardware state machine in the CAM based on the configuration information, wherein the hardware state machine comprises custom logic that is used to control access to the digital services and wherein the hardware state machine is not directly accessible to a system input/output module or system bus of the CAM, and wherein the custom logic block comprises a dedicated hardware reconfiguration and input/output module that connects the hardware state machine to a system bus of the CAM and controls access to logic of the hardware state machine.

2. (ORIGINAL) The system of claim 1 wherein the CAM comprises a smart card.

3. (ORIGINAL) The system of claim 1 wherein the configuration information is encrypted.

4. (ORIGINAL) The system of claim 3 wherein the configuration information is encrypted through a key exchange protocol.

5. (ORIGINAL) The system of claim 4 wherein the key exchange protocol comprises a public key algorithm.

6. (ORIGINAL) The system of claim 3 wherein the configuration information is received in uniquely encrypted, group encrypted packets.

7. (ORIGINAL) The system of claim 3 wherein the custom logic block is further configured to:

decrypt the configuration information; and

store the configuration information in one or more protected registers.

8. (ORIGINAL) The system of claim 1 wherein the custom logic block is further configured to verify that the configuration information is authentic.

9. (ORIGINAL) The system of claim 8 wherein the custom logic block is further configured to retain the configuration information if the configuration information is authentic.

10. (ORIGINAL) The system of claim 1 wherein the custom logic block is further configured to receive a synchronous command to reconfigure the hardware state machine using the configuration information.

11. (CANCELLED)

12. (ORIGINAL) The system of claim 1 wherein the custom logic block comprises an asynchronous dynamic pre-permutation module that employs a series of one or more configurable multiplexors at the beginning of the hardware state machine.

13. (ORIGINAL) The system of claim 1 wherein the custom logic block comprises an asynchronous dynamic post-permutation module that employs a series of one or more configurable multiplexors at the end of the hardware state machine.

14. (CANCELLED)

15. (CURRENTLY AMENDED) A method for providing access to digital services comprising:

(a) receiving configuration information in a security component comprising a smart card, wherein:

(1) the configuration information has been transmitted asynchronously; and

(2) the security component is configured to control access to the digital services; and

(b) dynamically reconfiguring a hardware state machine in the security component based on the configuration information, wherein the hardware state machine comprises custom logic that is used to control access to the digital services, and wherein a component of the hardware state machine is not directly accessible to a system input/output module or system bus of the security component, and wherein the custom logic comprises a dedicated hardware reconfiguration and input/output module that connects the hardware state machine to a system bus of the CAM and controls access to logic of the hardware state machine.

16. (CANCELLED)

17. (PREVIOUSLY PRESENTED) The method of claim 15 wherein the configuration information is received through a broadcast stream, Internet, or callback.

18. (ORIGINAL). The method of claim 15 wherein the configuration information is encrypted.

19. (ORIGINAL) The method of claim 18 wherein the configuration information is encrypted through a key exchange protocol.

20. (ORIGINAL) The method of claim 19 wherein the key exchange protocol comprises a public key algorithm.

21. (ORIGINAL) The method of claim 18 wherein the configuration information is received in uniquely encrypted, group encrypted packets.

22. (ORIGINAL) The method of claim 18 further comprising:

decrypting the configuration information; and

storing the configuration information in one or more protected registers.

23. (ORIGINAL) The method of claim 15 further comprising verifying the configuration information is authentic.

24. (ORIGINAL) The method of claim 23 further comprising retaining the configuration information if the configuration information is authentic.

25. (ORIGINAL) The method of claim 15 further comprising receiving a synchronous command to reconfigure the hardware state machine using the configuration information.

26. (CANCELLED)

27. (ORIGINAL) The method of claim 15 wherein the dynamic reconfiguration of the hardware state machine reconfigures a permutation that employs a series of one or more configurable multiplexors at the beginning of the hardware state machine.

28. (ORIGINAL) The method of claim 15 wherein the dynamic reconfiguration of the hardware state machine reconfigures a permutation that employs a series of one or more configurable multiplexors at the end of the hardware state machine.

29. (CANCELLED)

30. (CURRENTLY AMENDED) A system for providing access to digital services comprising:

(a) a conditional access module (CAM) configured to receive configuration information for accessing the digital services, wherein the configuration information has been transmitted asynchronously; and

(b) a custom logic block configured to dynamically reconfigure a hardware state machine in the CAM based on the configuration information, wherein the hardware state machine comprises custom logic that is used to control access to the digital services, and wherein a component of the

hardware state machine is not directly accessible to a system input/output module or system bus of the CAM, and wherein the custom logic block comprises a dedicated hardware reconfiguration and input/output module that connects the hardware state machine to a system bus of the CAM and controls access to logic of the hardware state machine.

31. (ORIGINAL) The system of claim 30 wherein the CAM comprises a smart card.

32. (PREVIOUSLY PRESENTED) The system of claim 30 wherein the configuration information is received through a broadcast stream, Internet, or callback.

33. (ORIGINAL) The system of claim 30 wherein the configuration information is encrypted.

34. (ORIGINAL) The system of claim 33 wherein the configuration information is encrypted through a key exchange protocol.

35. (ORIGINAL) The system of claim 34 wherein the key exchange protocol comprises a public key algorithm.

36. (ORIGINAL) The system of claim 33 wherein the configuration information is received in uniquely encrypted, group encrypted packets.

37. (ORIGINAL) The system of claim 33 wherein the custom logic block is further configured to:

decrypt the configuration information; and

store the configuration information in one or more protected registers.

38. (ORIGINAL) The system of claim 30 wherein the custom logic block is further configured to verify that the configuration information is authentic.

39. (ORIGINAL) The system of claim 38 wherein the custom logic block is further configured to retain the configuration information if the configuration information is authentic.

40. (ORIGINAL) The system of claim 30 wherein the custom logic block is further configured to receive a synchronous command to reconfigure the hardware state machine using the configuration information.

41. (CANCELLED)

42. (ORIGINAL) The system of claim 30 wherein the custom logic block comprises an asynchronous dynamic pre-permutation module that employs a series of one or more configurable multiplexors at the beginning of the hardware state machine.

43. (ORIGINAL) The system of claim 30 wherein the custom logic block comprises an asynchronous dynamic post-permutation module that employs a series of one or more configurable multiplexors at the end of the hardware state machine.

44. (CANCELLED)

45. (CURRENTLY AMENDED) An article of manufacture for providing access to digital services comprising:

(a) means for receiving configuration information in a security component comprising a smart card, wherein:

(1) the configuration information has been transmitted asynchronously; and

(2) the security component is configured to control access to the digital services; and

(b) means for dynamically reconfiguring a hardware state machine in the security component based on the configuration information, wherein the hardware state machine comprises custom logic that is used to control access to the digital services, and wherein a component of the hardware state machine is not directly accessible to a system input/output module or system bus of the security component, and wherein the custom logic comprises a dedicated hardware reconfiguration and input/output module that connects the hardware state machine to a system bus of the CAM and controls access to logic of the hardware state machine.

46. (CANCELLED)

47. (PREVIOUSLY PRESENTED) The article of manufacture of claim 45 wherein the configuration information is received through a broadcast stream, Internet, or callback.

48. (ORIGINAL) The article of manufacture of claim 45 wherein the configuration information is encrypted.

49. (ORIGINAL) The article of manufacture of claim 48 wherein the configuration information is encrypted through a key exchange protocol.

50. (ORIGINAL) The article of manufacture of claim 49 wherein the key exchange protocol comprises a public key algorithm.

51. (ORIGINAL) The article of manufacture of claim 48 wherein the configuration information is received in uniquely encrypted, group encrypted packets.

52. (ORIGINAL) The article of manufacture of claim 48 further comprising:
means for decrypting the configuration information; and
means for storing the configuration information in one or more protected registers.

53. (ORIGINAL) The article of manufacture of claim 45 further comprising means for verifying the configuration information is authentic.

54. (ORIGINAL) The article of manufacture of claim 53 further comprising means for retaining the configuration information if the configuration information is authentic.

55. (ORIGINAL) The article of manufacture of claim 45 further comprising means for receiving a synchronous command to reconfigure the hardware state machine using the configuration information.

56. (CANCELLED)

57. (ORIGINAL) The article of manufacture of claim 45 wherein the dynamic reconfiguration of the hardware state machine reconfigures a permutation that employs a series of one or more configurable multiplexors at the beginning of the hardware state machine.

58. (ORIGINAL) The article of manufacture of claim 45 wherein the dynamic reconfiguration of the hardware state machine reconfigures a permutation that employs a series of one or more configurable multiplexors at the end of the hardware state machine.

59. (CANCELLED)

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.